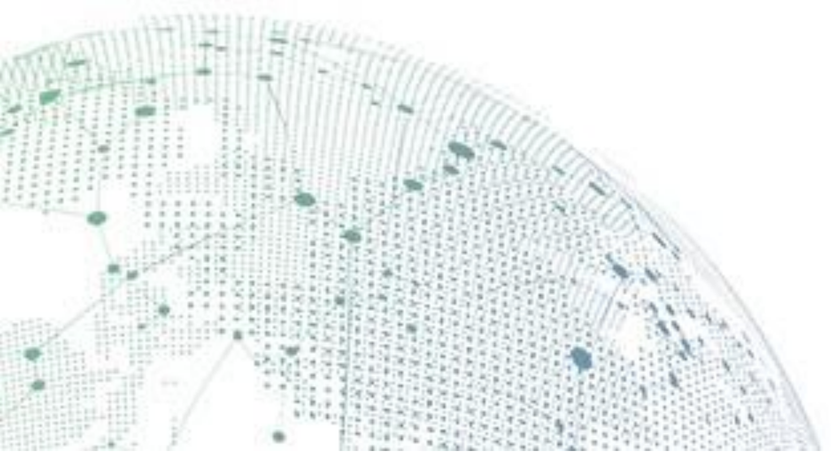
NGAF

APT related issues Troubleshooting

Version 8.0.6



Change Log

Date	Change Description
May 2, 2019	APT related issues Troubleshooting

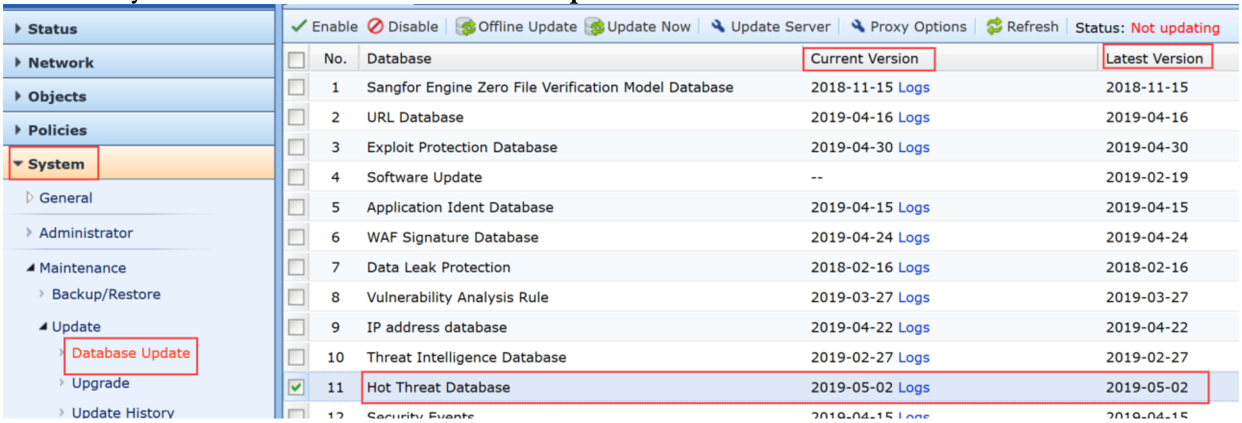
Content

Chapter 1 Application scenario

APT related issuesTroubleshooting

Chapter 2 Troubleshooting methods

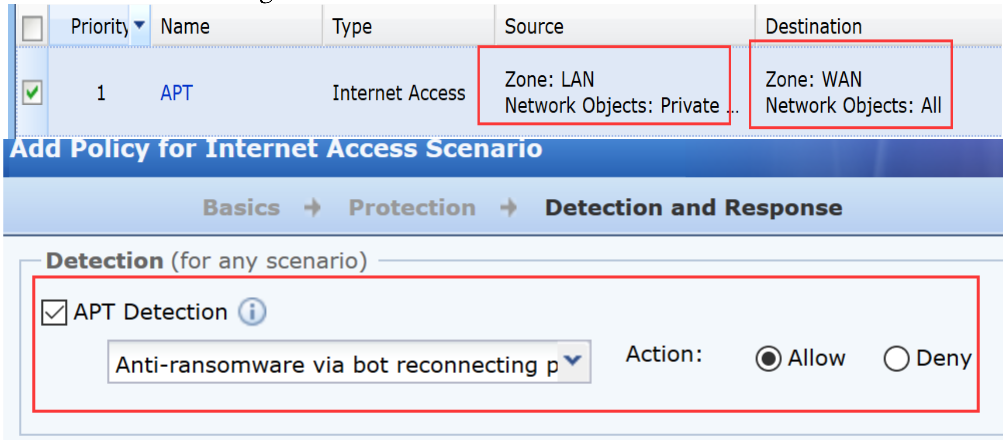
1. Go to **System** > **Maintenance** > **Database Update** check if the Hot Threat Database is Latest Version.



Status: Not updating

No.	Database	Current Version	Latest Version
1	Sangfor Engine Zero File Verification Model Database	2018-11-15 Logs	2018-11-15
2	URL Database	2019-04-16 Logs	2019-04-16
3	Exploit Protection Database	2019-04-30 Logs	2019-04-30
4	Software Update	--	2019-02-19
5	Application Ident Database	2019-04-15 Logs	2019-04-15
6	WAF Signature Database	2019-04-24 Logs	2019-04-24
7	Data Leak Protection	2018-02-16 Logs	2018-02-16
8	Vulnerability Analysis Rule	2019-03-27 Logs	2019-03-27
9	IP address database	2019-04-22 Logs	2019-04-22
10	Threat Intelligence Database	2019-02-27 Logs	2019-02-27
☑ 11	Hot Threat Database	2019-05-02 Logs	2019-05-02
12	Security Events	2019-04-15 Logs	2019-04-15

2. Go to **Policies** > **Network Security** > **Policies** check if the policies is configured APT Detection, Then check if the zone configuration is correct.



Priority	Name	Type	Source	Destination
☑ 1	APT	Internet Access	Zone: LAN Network Objects: Private ..	Zone: WAN Network Objects: All

Add Policy for Internet Access Scenario

Basics → Protection → Detection and Response

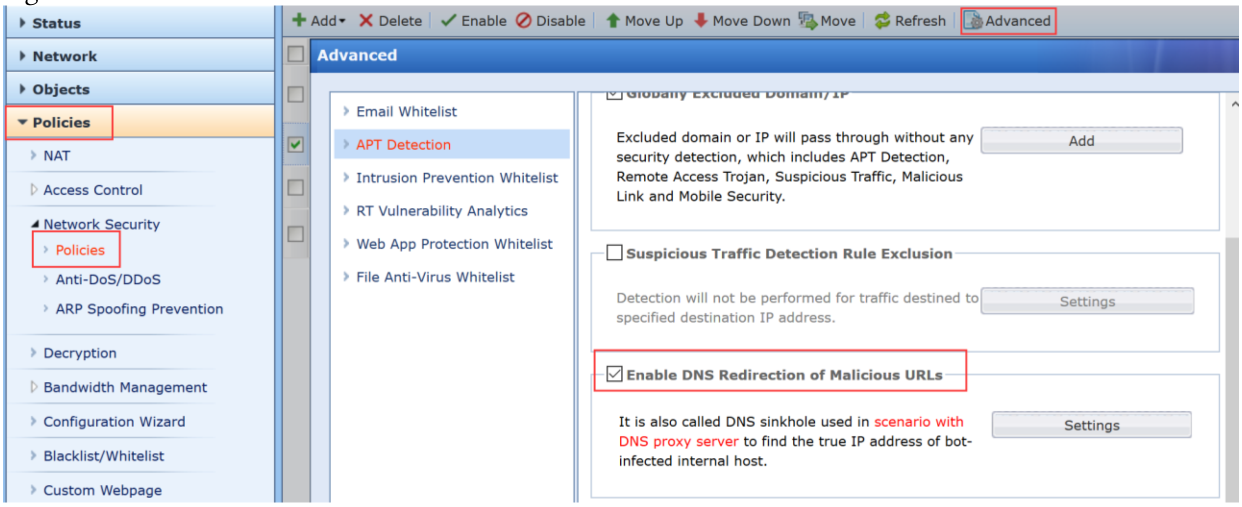
Detection (for any scenario)

☑ APT Detection

Anti-ransomware via bot reconnecting p

Action: ● Allow ○ Deny

3. Once it is enabled in User scenario, servers in destination zone will be detected for virus, Trojan, etc., however, if DNS proxy is enabled, it it better to enable DNS redirection of malicious URLs. After enbale the DNS redirection, we will be able to see the intranet computer IP instead of the proxy server IP in the APT log.



Advanced

☑ Globally Excluded Domain/IP

Excluded domain or IP will pass through without any security detection, which includes APT Detection, Remote Access Trojan, Suspicious Traffic, Malicious Link and Mobile Security. Add

□ Suspicious Traffic Detection Rule Exclusion

Detection will not be performed for traffic destined to specified destination IP address. Settings

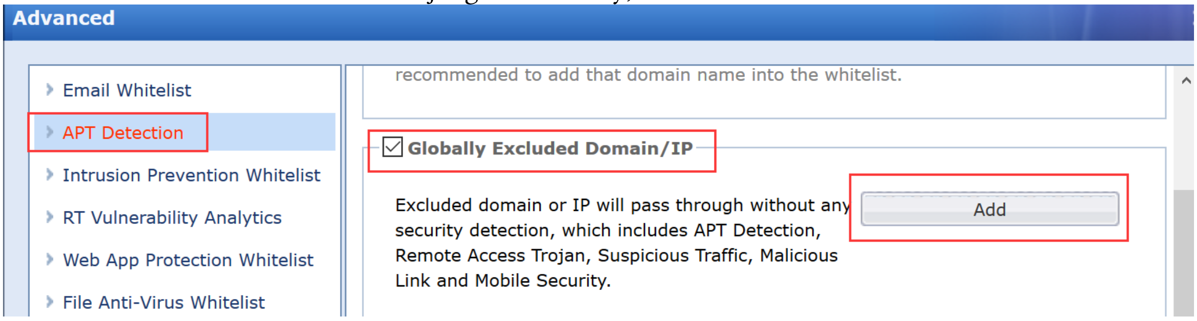
☑ Enable DNS Redirection of Malicious URLs

It is also called DNS sinkhole used in scenario with DNS proxy server to find the true IP address of bot-infected internal host. Settings

4. Go to **System** > **Troubleshooting** check if Start Bypass.

5. Go to **Policies** > **Blacklist/Whitelist** check if the whitelist matches the corresponding IP.

6. Go to **Policies** >**Network Security** > **Policies** >**Advanced** check if there is enable Globally Excluded Domain/IP. If it is found that the misjudgment is deny, we can add Domain/IP here.


Advanced
Email Whitelist
APT Detection
Intrusion Prevention Whitelist
RT Vulnerability Analytics
Web App Protection Whitelist
File Anti-Virus Whitelist
Add

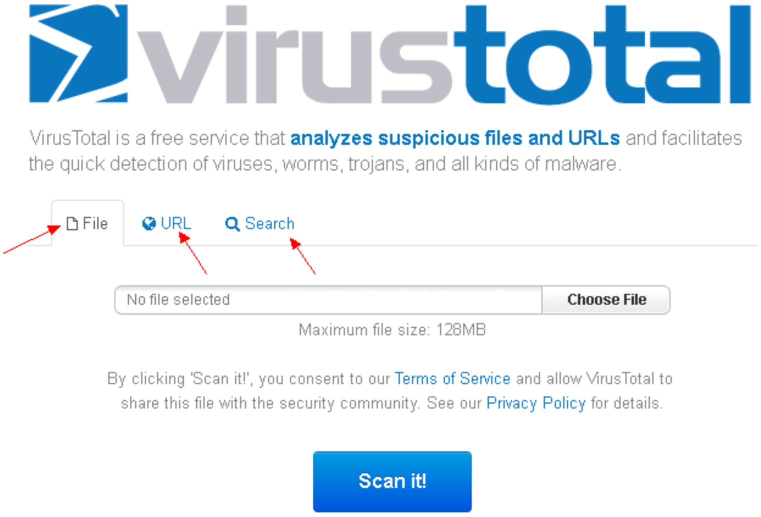
recommended to add that domain name into the whitelist.

☑ Globally Excluded Domain/IP

Excluded domain or IP will pass through without any security detection, which includes APT Detection, Remote Access Trojan, Suspicious Traffic, Malicious Link and Mobile Security.

7. If a computer confirms that it is infected with a botnet, we can use **Sangfor Anti-Bot Tool** to handle it. The specific download address of the tool: **http://go.sangfor.com/edr-tool-20180824.** The tool is only for windows system, if it is Linux system, you can search for related tools online.

8. VirusTotal is an internationally renowned suspicious file and web analytics service website. You can use this website to judge whether the relevant documents or websites are malicious. Website specific access address: https://www.virustotal.com/ . There are some abnormal links that cannot be confirmed, which need to be analyzed in detail in conjunction with the business situation.



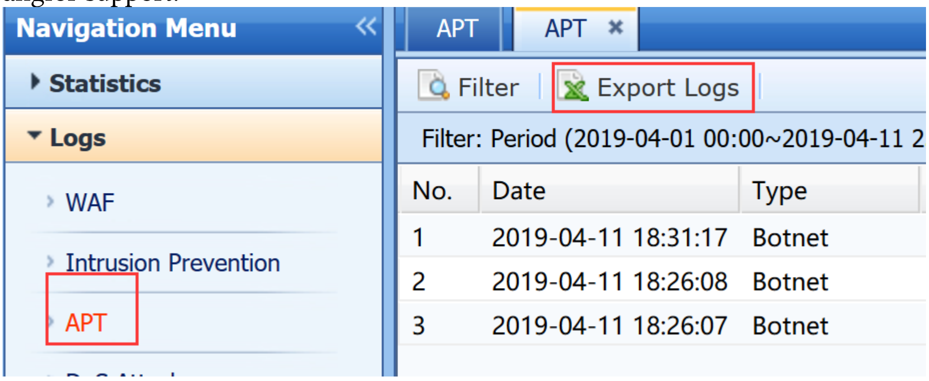
VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

9. If the above troubleshooting does not solve the problem, you can export the APT logs to contact sangfor support.



Filter: Period (2019-04-01 00:00~2019-04-11 2

No.	Date	Type
1	2019-04-11 18:31:17	Botnet
2	2019-04-11 18:26:08	Botnet
3	2019-04-11 18:26:07	Botnet

SANGFOR

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc